Operating System

Windows 2000 Reliability and Availability Improvements

White Paper

Abstract

The Microsoft® Windows® 2000 operating system was designed to address hardware, software, and system management issues that affect reliability and availability.

Microsoft added many features and capabilities to Windows 2000 to increase reliability and availability. In addition, Microsoft enhanced the development and testing process to ensure that Windows 2000 is a highly dependable operating system. This paper provides a technical introduction to these improvements and new features and explains how reliability and availability are improved in Windows 2000 Advanced Server and Windows 2000 Datacenter Server. It shows how organizations can employ a coordinated strategy that maximizes the benefits of using the right technology in conjunction with support programs, investments in properly trained or certified personnel, and adoption of prescriptive guidelines for efficiently operating the OS.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved. Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

9/2000

Contents

Executive Summary.....1

Using the right technology 1

How Advanced Server Increases Availability 2

Increasing Server Availability 2

How Datacenter Server Increases Reliability and Availability 2

Maximizing Availability with 32 SMP and 4-Node Clustering 3

High Performance with Winsock Direct 3

Managing Critical Resources with the Process Control Tool 3

Using Services and Support Programs 3

Windows 2000 Datacenter Program 4

Investing in People and Process 4

Microsoft Operations Framework: Roadmap for Reliability 4

Investing in properly trained or certified personnel 4

Microsoft Readiness Framework (MRF) 5

Microsoft Certification 5

Conclusion 5

Introduction.....6

Coordinating Strategy for Reliability and Availability 6

Preparing for Windows 2000 Dependability.....7

Building Dependability in Windows 2000.....8

The Windows 2000 development process 8

Using the Right Technology.....9

Reliability and Availability Features in the Windows 2000 Server Family 9

Architectural Improvements 9

Windows File Protection 9

Kernel-Mode Write Protection 10

Reducing the number of reboot conditions 11

Improved Tools for Third Parties 11

Service Pack Slipstreaming 11
Reducing recovery time 12
Recovery Console 12
Safe Mode Boot 13
Kill Process Tree 13
Recoverable File System 13
Automatic Restart 13
IIS Reliable Restart 14
Storage management 14
Improved diagnostic tools 15
Kernel-Only Crash Dumps 15
Mini Dumps 15
Faster CHKDSK 16
MSINFO 16
Remote Terminal Services 16

Windows 2000 Advanced Server Availability Features..17
Symmetric multiprocessing (SMP) 17
Clustering 17
Network Load Balancing 17
Component Load Balancing 18

Windows 2000 Datacenter Server Reliability and Availability Improvements.....20
Maximizing Availability: 32 SMP and 4-Node Clustering 20
High Performance with Winsock Direct 20
Managing Critical Resources: The Process Control Tool 20

Using Services and Support Programs.....22
Assisted Support Options for Organizations 23
Windows 2000 Datacenter Program 23
OEM/Microsoft Jointly Staffed Support Queue 24
Hardware Compatibility Test & List 25

The Role of Windows Hardware Quality Labs 26
Ongoing Testing Requirements 26
Datacenter Planning 27
Windows 2000 Datacenter Program Servers 27
Software Maintenance 28

People and Process.....29
Microsoft Operations Framework: Roadmap for Reliability 29
Building on Standardized Best Practices 29
Enterprise Services Frameworks 29
Principles of MOF 30
The MOF Process Model 31
Investing in properly trained or certified personnel 33
Microsoft Readiness Framework 33
Microsoft Certification 34

Conclusion.....35

Appendix A: Reduced Reboot Scenarios.....36
File system maintenance 36
Hardware installation and maintenance 36
Networking and communications 36
Memory management 37
Software installation 37
Performance tuning 37

Appendix B: Tools for Third Parties.....38
Kernel-Mode Code Development 38
Driver Signing 40
Developing and debugging user-mode code 41

For More Information.....42

Executive Summary

In the increasingly competitive global marketplace of e-commerce, a fairly simple law dictates who wins and who loses. If your system is available, you're ready to do business with partners and customers. But if your system is down, employees aren't working, partners are shut out, and customers are turned away. The stakes for maintaining reliable, Internet-enabled networks have never been higher.

Building maximum reliability and availability into the OS was one of the most important goals in the development of Windows 2000. Understanding how to make these new features work for you is the subject of this paper.

This paper highlights the reliability and availability features integrated throughout the Windows 2000 Server family of operating systems. It shows how you can achieve greater availability using the clustering and load balancing features in Windows 2000 Advanced Server. Then, it explains how Windows 2000 Datacenter Server expands on these features to deliver an operating system that meets the highest levels of reliability and availability.

But achieving optimum reliability and availability in an enterprise environment requires more than just adopting the latest technology. Studies show that as much as 80 percent of system failures can be traced to errors caused by people or flawed processes. Therefore, organizations need to employ a coordinated strategy that maximizes the benefits of using the right technology in conjunction with the following:

- Support programs providing expertise from Microsoft and/or vendors.
- Investments in properly trained or certified administrators.
- Adoption of prescriptive guidelines for efficiently operating the OS.

This section provides a high level summary of these essential features, which are explained in more depth later in this paper.

Using the right technology

Keeping your systems up and running begins with technology. The Microsoft Windows 2000 Server family of operating systems share a core set of architectural features aimed at ensuring continued reliability and availability.

- **Improved Internal Architecture.** Windows 2000 includes new features designed to protect your system, such as preventing new

software installations from replacing essential system files or stopping applications from writing into the kernel of the OS. This greatly reduces many of the sources of operating system corruption and failure.

- **Fast Recovery from System Failure.** If your system does fail, Windows 2000 includes an integrated set of features designed to quickly restore your system.
- **Improved Code with Developer Tools.** Microsoft provided third-party developers with tools and programs to improve the quality of their drivers, system level programs, and application code. These enhancements make it easier for independent software vendors to write dependable code for Windows 2000.
- **Reduced Reboot Scenarios.** Microsoft has greatly reduced the number of operations requiring a system reboot in almost every category of OS functionality: file system maintenance, hardware installation and maintenance, networking and communications, memory management, software installation, and performance tuning.

How Advanced Server Increases Availability

The Windows 2000 Advanced Server operating system contains all the functionality and reliability of Windows 2000 Server, plus additional features for applications that require higher levels of scalability and availability.

Windows 2000 Advanced Server lets you readily increase your server capacity to keep pace with business growth, and it increases the availability of your important systems.

Increasing Server Availability

Server downtime caused by hardware or software failures can result in lost revenue, wasted IT staff work, and unhappy customers. To address these concerns, there are two kinds of technology used to increase server availability in Windows 2000 Advanced Server: Windows Clustering and Network Load Balancing (NLB).

Windows Clustering links individual servers so they can perform common tasks. If one server stops functioning, two-node failover-support transfers its workload to the other server. Network Load Balancing uses 8-way symmetric multiprocessing (SMP) to ensure a server is always available to handle requests on your Web site or communications network. NLB works by spreading client requests

among various servers that are linked together to support a particular application.

Windows 2000 Advanced Server lets you sustain productivity and ensure customer satisfaction by increasing the load your server infrastructure can reliably handle.

How Datacenter Server Increases Reliability and Availability

Only original equipment manufacturers (OEMs) that meet a stringent set of hardware and software guidelines can offer Windows 2000 Datacenter Server. This certification requirement combined with the most advanced reliability and availability features delivers an OS designed to meet the needs of large data warehouses, online transaction processing (OLTP), large-scale simulations in science and engineering, and server consolidation.

Windows 2000 Datacenter Server includes all the features in Advanced Server and adds expanded server capacity and clustering to maximize reliability and availability.

Maximizing Availability with 32 SMP and 4-Node Clustering
Datacenter Server increases symmetric multiprocessing (SMP) capacity to 32 CPUs per cluster compared with 8 CPUs in Advanced Server. This allows network administrators to take full advantage of Network Load Balancing (NLB) capability. Failover support is increased in Datacenter Server to support four nodes, compared with two nodes in Advanced Server.

High Performance with Winsock Direct
Winsock Direct enables efficient high-bandwidth, low-latency messaging that conserves processor time for application use. In system area networks (SAN), this allows more users on the system, providing faster response times and higher transaction rates.

Managing Critical Resources with the Process Control Tool
Process Control is a powerful, flexible tool that helps you manage and control the resources that processors use on your system by applying rules that you define. When adjusted to fit the design of an application, Process Control helps ensure predictable and stable operations.

Using Services and Support Programs

Maintaining optimum reliability and availability requires access to support professionals and programs specifically tailored for demanding business requirements. Microsoft offers a wide range of support programs aimed at ensuring maximum reliability and availability. For a complete summary of support options, see the Microsoft Support Web site at http://support.microsoft.com/directory/overview.asp.

Microsoft Certified Support Centers

Microsoft Certified Support Centers (MCSCs) are industry leading, multi-vendor support providers who have a special relationship with Microsoft that helps ensure they deliver high quality technical support for Microsoft products. All MCSCs possess significant industry expertise in many types of environments and can provide your organization with a broad range of life-cycle services and extended capabilities that form an economical and cohesive business solution. For more information on the support options available, see the Microsoft Certified Support Centers home page at http://www.microsoft.com/support/mcsc/

Windows 2000 Datacenter Program

The Windows 2000 Datacenter Program is designed to provide customers with an integrated hardware, software, and service offering—all delivered by Microsoft and qualified server vendors (OEMs). Three areas make up the program:

- **OEM/Microsoft Jointly Staffed Support Queue.** This gives partners access to the Microsoft resources they need to help customers achieve high levels of availability, and establishes a unique level of cooperation in delivering support for critical business systems. Customers can dial a single number to obtain this integrated support.
- **Hardware Compatibility Test & List.** OEM products must pass a special Hardware Compatibility Test (HCT) verifying that quality hardware and software interacts efficiently and optimally with Microsoft products.
- **Software Maintenance.** Customers can receive update subscriptions for access to version releases, supplements, and Service Packs for Datacenter Server.

Investing in People and Process

Microsoft Operations Framework: Roadmap for Reliability
Studies show that as much as 80 percent of system failures can be traced to errors caused by people or processes. Therefore, an essential part of reliability strategy is adopting prescriptive guidelines that cover the best practices that have been learned by enterprises over time. The Microsoft Operations Framework (MOF) provides technical guidance for achieving mission-critical production system reliability, availability, and manageability on Microsoft products and technologies.

Investing in properly trained or certified personnel

The potential for human error remains a significant roadblock in keeping your systems reliable and available. People may forget to perform backups or ignore proper procedures for performing a wide range of operational tasks. The lesson is clear: If your employees aren't properly trained to maintain your systems, you risk compromising the reliability and availability that you should be achieving. Two extensive programs exist to help you meet this goal: The Microsoft Readiness Framework and the Microsoft Certification Program.

Microsoft Readiness Framework (MRF)
MRF helps IT organizations develop individual and organizational readiness to use Microsoft's products and technologies. This guidance includes assessment and readiness planning tools, learning roadmaps, readiness-related white papers, self-paced training, courses, certification exams, and readiness events.

For more information about how MRF fits in with the Enterprise Services Framework, see the Enterprise Services home page at http://www.microsoft.com/msf.

Microsoft Certification
Competitive organizations are led at all levels by professionals who know technology and can innovate, take initiative, and think strategically. Microsoft certification can help organizations find these technical leaders. Microsoft certification is an objective way for businesses to identify individuals who have the technical abilities to help them compete in their industry and move forward with the most advanced Microsoft technology. Certification provides professionals with a credential that acknowledges their skills with Microsoft

products. For more information about Microsoft certification and other training opportunities, see the Microsoft Certification Web site at http://www.microsoft.com/trainingandservices/default.asp

Conclusion

The Windows 2000 Server product line is the most reliable set of server operating systems Microsoft has ever produced. The reliability improvements in Windows 2000 mean fewer network interruptions for end users, higher server uptime, and better availability.

Advanced Server meets the needs of essential business and e-commerce applications that handle heavier workloads and high-priority processes. You can readily increase your server capacity to keep pace with business growth while enhancing the availability of your important systems.

Windows 2000 Datacenter Server uses stringent standards for hardware and software configurations to deliver an OS designed to meet the highest demands for reliability and availability. It includes all features in Advanced Sever plus greater clustering, load balancing, memory support, process controls, and other features optimized to deliver the high availability and reliability required for enterprise and larger departmental solutions.

Obtaining optimum reliability and availability depends on investments in people and process, ensuring properly trained personnel follow prescriptive practices based on the Microsoft Operations Framework and the expertise provided by support programs.

Organizations must be able to depend on their business information systems to deliver consistent results. The foundation of all information systems—the operating system platform—provides dependability through two basic characteristics: *reliability* and *availability*.

Reliability refers to how consistently a server runs applications and services. Reliability is increased by reducing the potential causes of system failure. Increasing reliability also increases the time between failures.

Availability refers to the percentage of time that a system is available for users. Availability is increased by improving reliability and by reducing the amount of time that a system is down for other reasons, such as planned maintenance or recovery from failure.

In short, reliable and available systems resist failure and are quick to restart after they’ve been shut down.

Preparing for Windows 2000 Dependability

This paper presents the ways in which Windows 2000 has been shaped into an extremely reliable platform for highly available systems. It begins with a background discussion about the research and development efforts that Microsoft undertook to enhance reliability and availability and goes on to explain the new technical features introduced in the Windows 2000 Server family. The paper shows how availability is enhanced with Windows 2000 Advanced Server and explains why it is the OS for essential business and e-commerce applications that handle heavier workloads and high-priority processes. The technical section concludes with a description of the benefits of Windows 2000 Datacenter Server, explaining how it meets the demands of the most intensive applications and large-scale environments.

Coordinating Strategy for Reliability and Availability

Achieving optimum reliability in an enterprise environment requires coordinating the following elements of a reliability strategy:

- Using the right technology.
- Taking advantage of services and support programs.
- Ensuring personnel have the skills and/or certification to maximize reliability and availability features.
- Using cost-effective, prescriptive processes to operate the OS.

The operating system is the core of any business computing system. Windows 2000 is the most dependable operating system ever produced by Microsoft.

The first step in making Windows 2000 an extremely dependable operating system was to discover ways that its predecessor, the Windows NT® operating system could be improved. Microsoft worked with a large body of data collected internally and from customers to identify areas of improvement for Windows NT 4.0.

As a result of this research, Microsoft developed a number of dependability requirements for Windows 2000:

- Increased reliability by reducing the number of system failures through extensive code review and testing.

Building Dependability in Windows 2000

- Increased availability by reducing the number of conditions that forced an operator to reboot the server, speeding recovery time.
- An improved installation procedure by preventing crucial system files from being overwritten.
- Improved device drivers, which were frequently the source of system failure.
- Better tools to help developers create dependable system software.
- Better tools for diagnosing potential causes of system failures.
- Improved tools for storage management.

Research also showed a need for Microsoft to guide customers in selecting hardware and software for assembling highly dependable systems.

Windows 2000 has met and exceeded all of these goals with the features and processes described in this paper.

Dependability is not a quality that can be dramatically improved by just adding features. Microsoft also improved the entire process of developing Windows 2000 internally, as well as offering a program for original equipment manufacturers (OEMs) to certify their systems as dependable.

The Windows 2000 development process

An operating system is a highly complex piece of software. The operating system must respond to a wide range of user requests and conditions under wildly varying usage scenarios.

Microsoft began the process of increasing the reliability of Windows 2000 by conducting extensive interviews with existing customers to identify some of the problems with previous versions of Windows that led to reduced system reliability.

Then Microsoft implemented internal reliability improvement practices during the development process, such as a full-time source code review team, whose sole responsibility was to double check the validity of the actual operating system code itself.

Using the Right Technology

Windows 2000 also underwent an incredibly rigorous testing process. Microsoft devoted more than 500 person years and more than $162 million dollars in testing and verifying Windows 2000 during its development cycle. The testing process itself was improved. Comprehensive system component tests were run, and a 'stress test' on more than 1,000 machines was run on a nightly basis. In addition, 100 servers were used for long-term testing of client-server systems.

Some of the highlights of the testing process include:

- More than 1,000 testers who used over 10 million lines of testing code.
- More than 60 test scenarios, such as using Windows 2000 as a print server, an application server, and a database server platform.
- Backup and restore testing of more than 88 terabytes of data each month.
- 130 domain controllers in a single domain.
- More than 1,000 applications tested for compatibility.

This virtually unprecedented testing process has resulted in the delivery of a highly stable and dependable operating system platform.

Reliability and Availability Features in the Windows 2000 Server Family

Microsoft has enhanced the dependability of Windows 2000 in a number of ways:

- Improved the internal architecture of Windows 2000.
- Provided third-party developers with tools and programs to improve the quality of their drivers, system level programs, and application code.
- Reduced the number of maintenance operations that require a system reboot.
- Allowed Service Packs to be easily added to existing installations.
- Reduced the time it takes to recover from a system failure.

- Added tools for easier storage management and improved diagnosis of potential problem conditions.

Users can also take advantage of clustering and load balancing, which are key features for implementing highly available systems.

Architectural Improvements

The internal architecture of Windows 2000 has been modified to increase the reliability of the operating system. The enhanced reliability stems from improvements in the protection of the operating system itself and the ability to protect shared operating system files from being overwritten during the installation of new software.

Windows File Protection

Before Windows 2000, installing new software could overwrite shared system files such as DLL and executable files. Because most applications use many different DLLs and executables, replacing existing versions of these system files can cause system performance to become unpredictable: applications can perform erratically or the operating system can fail.

Windows File Protection verifies the source and version of a system file before it is initially installed. This verification prevents the replacement of protected system files with extensions such as .sys, .dll, .ocx, .ttf, .fon, and .exe files. Windows File Protection runs in the background and protects all files installed by the Windows 2000 setup program. It detects attempts by other programs to replace or move a protected system file. Windows File Protection also checks a file's digital signature to determine if the new file is the correct Microsoft version.

If the file is not the correct version, Windows File Protection replaces the file from the backup stored in the Dllcache folder, network-install location, or from the Windows 2000 CD. If Windows File Protection cannot locate the appropriate file, it prompts the user for the location. Windows File Protection also writes an event noting the file replacement attempt to the event log.

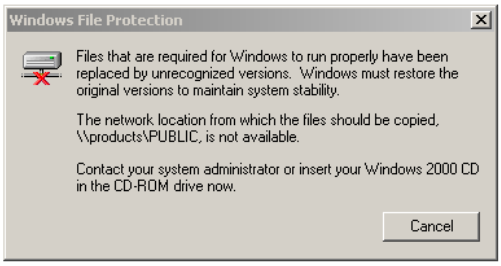
Windows File Protection
Files that are required for Windows to run properly have been replaced by unrecognized versions. Windows must restore the original versions to maintain system stability.
The network location from which the files should be copied, \\products\PUBLIC, is not available.
Contact your system administrator or insert your Windows 2000 CD in the CD-ROM drive now.
Cancel

Figure 1: Users will be warned if an application tries to write over files that are part of the Windows-based operating system.

By default, Windows File Protection is always enabled and only allows protected system files to be replaced when installing the following:

- Windows 2000 Service Packs using Update.exe.
- Hotfix distributions using Hotfix.exe.
- Operating system upgrades using Winnt32.exe.
- Windows Update.
- Windows 2000 Device Manager/Class Installer.

Kernel-Mode Write Protection

Another important write-protection feature in Windows 2000 is designed to protect the kernel from any errant code, “rogue” applications, or other interference.

Windows 2000 is made up of a variety of small, self-contained software components that work together to perform tasks. Each component provides a set of functions that act as an interface to the rest of the system. This collection of components allows access to the processor and all other hardware resources.

Windows 2000 divides these components into two basic modes—kernel mode and user mode. User mode is the portion of the operating system in which application software runs. Kernel mode is the portion that interacts with computer hardware.

In kernel-mode, software can access all the resources of a system, such as computer hardware and sensitive system data. Before Windows 2000, code running in kernel-mode was not protected from

being overwritten by errant pieces of other kernel-mode code, while code running in user-mode programs or dynamic-link libraries (DLL) was either write-protected or marked as read-only. Windows 2000 adds this protection for subsections of the kernel and device drivers, which reduces the sources of operating system corruption and failure.

To provide this new protection, hardware memory mapping marks the memory pages containing kernel-mode code, ensuring they cannot be overwritten, even by the operating system. This prevents kernel-mode software from silently corrupting other kernel-mode code. If a piece of code attempts to modify protected areas in the kernel or device drivers, the code will fail. Making code failures much more obvious makes it more likely that defects in kernel-mode code will be found during development. This feature is turned on by default, although it can be deactivated if a developer desires to do so.

Reducing the number of reboot conditions

As described earlier in this paper, there is a difference between reliability and availability. A system can be running reliably, but if a maintenance operation requires that the system be taken down and restarted, the availability of the system is compromised. For users, it makes no difference whether the system is down for a planned maintenance operation or a hardware failure: they cannot use the system in either case.

Windows 2000 has greatly reduced the number of operations that require a system reboot in major categories of OS functionality: file system maintenance, hardware installation and maintenance, networking and communications, memory management, software installation, and performance tuning. See Appendix A for a list of the tasks that can be completed without interruption.

Improved Tools for Third Parties

Windows 2000 also provides a number of tools and features that make it easier for independent software vendors to write dependable code for Windows 2000. For a detailed discussion of how these tools contribute to enhanced reliability and availability, see Appendix B.

Service Pack Slipstreaming

Microsoft periodically releases Service Packs, which offer software improvements and enhancements. These updates can be slipstreamed into the base operating system, freeing users from having to reinstall a Service Pack after installing new components. Slipstreaming automates the Service Pack deployment process allowing users to install the latest Service Pack from a single share so

that when setup runs, the right files and registry entries are always used. This feature allows customers to build their own packages for Windows 2000, with the appropriate Service Pack and/or hotfixes—customizing the OS to meet specific organizational needs.

Reducing recovery time

One of the differences between reliability and availability stems from the time it takes for a system to recover from a failure. Although a system may begin to run reliably as soon as it is restarted, the system is usually not available to users until a number of corrective processes have run their course. The longer it takes to recover from a system failure, the lower the availability of the system.

A number of improvements in Windows 2000 help reduce the amount of time it takes to recover from a system failure and restart the operating system. These improvements include:

- Recovery Console
- Safe Mode Boot
- Kill Process Tree
- Recoverable File System
- Automatic Restart
- IIS Reliable Restart

Recovery Console

In the event of a system failure, administrators must be able to rapidly recover the system. The Windows 2000 Recovery Console is a command-line console utility available to administrators from the Windows 2000 Setup program. It can be run from text-mode setup using the Windows 2000 CD or system disk (boot floppy).

The Recovery Console is particularly useful for repairing a system by copying a file from a floppy disk or CD-ROM to the hard drive, or for reconfiguring a service that is preventing the computer from starting properly. Using the console, users can start and stop services, format drives, read and write data on a local drive, including drives formatted to use the NTFS file system, and perform many other administrative tasks.

Because the Recovery Console allows users to read and write NTFS volumes using the Windows 2000 boot floppy, it will help organizations reduce or eliminate their dependence on FAT and DOS

boot floppies used for system recovery. In addition, it provides a way for administrators to access and recover a Windows 2000 installation, regardless of which file system has been used (FAT, FAT32, NTFS), with a set of specific commands. At the same time, the Recovery Console preserves Windows 2000 security, since a user must log onto the Windows 2000 system to access the console and the requested installation feature.

While using the Recovery Console, files cannot be copied from the system to a floppy or other form of removable media, which eliminates a potential source of accidental or malicious corruption of the system or breaches in data security.

Safe Mode Boot

To help users and administrators diagnose system problems such as errant device drivers, the Windows 2000 operating system can be started using Safe Mode Boot. In Safe Mode, Windows 2000 uses default hardware settings for items such as mouse, monitor, keyboard, mass storage, base video, default system services, and no network connection. Booting in Safe Mode allows users to change the default settings or remove a newly installed driver that is causing a problem.

In addition to Safe Mode options, users can select Step-by-Step Configuration Mode, which lets them choose the basic files and drivers to start, or the Last Known Good Configuration option, which starts their computer using the registry information that Windows saved at the last shutdown.

Kill Process Tree

If an application stops responding to the system, users need a way to stop the application. A user could simply stop the main process for the application, but a process could have spawned many other processes, which could have spawned child processes of their own, and so on—resulting in a tree of processes all logically descended from one top-level program.

For this reason, Windows 2000 provides the Kill Process Tree utility, which allows Task Manager to stop not only a single process, but also any processes created by that parent process with a single operation. The Kill Process Tree utility does not require a system reboot. The Kill Process Tree utility is especially useful in cases where a process has created many other processes, which, in turn, have caused a reduction in overall system performance.

Recoverable File System

The Windows 2000 file system (NTFS) is highly tolerant of disk failures because it logs all disk I/O operations as unique transactions. In the event of a disk failure, the file system can quickly undo or redo transactions as appropriate when the system is brought back up. This reduces the time the system is unavailable since the file system can quickly return to a known, functioning state.

Automatic Restart

The improvements in Windows 2000 reduce the likelihood of system failures. However, if a failure does occur, the system can be set to restart itself automatically. This feature provides maximum unattended uptime.

When an automatic restart occurs, memory contents can be written to a log file before restart to assist the administrator in determining the cause of the failure.

IIS Reliable Restart

In the past, to reliably restart Internet Information Server (IIS) by itself, an administrator needed to restart up to four separate services. This recovery process required the operator to have specialized knowledge to accomplish the restart, such as the syntax of the Net command. Because of this complexity, rebooting the entire operating system was the typical, although not optimal, way to restart IIS.

To avoid this interruption in the availability of the system, Windows 2000 includes IIS Reliable Restart, a faster, easier, and more flexible one-step-restart process. The user can restart IIS by right-clicking an item in the Microsoft Management Console (MMC) or by using a command-line application. For greater flexibility, the command-line application can also be executed by other Microsoft and third-party tools, such as HTTP-Mon and the Windows 2000 Task Scheduler. IIS will use the Windows 2000 Service Control Manager's functionality to automatically restart IIS Services if the INETINFO process terminates unexpectedly or crashes.

Storage management

Storage requirements tend to continually increase for servers. To avoid system problems resulting from users running out of disk space, Windows 2000 provides several enhancements for storage management to help administrators maintain sufficient free disk space with minimal effort. Storage management features in Windows 2000 include:

- **Remote Storage Services.** The Remote Storage Services (RSS) monitors the amount of space available on a local hard disk. When the free space on a primary hard disk dips below the needed level, RSS automatically removes local data that has been copied to remote storage, providing the free disk space needed.
- **Removable Storage Manager.** The Removable Storage Manager (RSM) presents a common interface to robotic media changers and media libraries. It allows multiple applications to share local libraries and tape or disk drives, and controls removable media within a single-server system.
- **Disk Quotas.** Windows 2000 Server supports disk quotas for monitoring and limiting disk space use on NTFS volumes. The operating system calculates disk space use for users based on the files and folders that they own. Disk space allocations are made by applications based on the amount of disk space remaining within the user's quota.
- **Dynamic Volume Management.** Dynamic Volume Management allows online administrative tasks to be performed without shutting down the system or interrupting users.

Improved diagnostic tools

Whenever a condition occurs that leads to a system failure, an administrator should try and determine the root cause of the problem in order to take preventative steps to avoid the problem in the future. Windows 2000 includes three new features for improving the ability to troubleshoot system errors:

- Kernel-only crash dumps
- Mini dumps
- Faster CHKDSK
- MSINFO
- Remote Terminal Services

Kernel-Only Crash Dumps

In the unlikely event that a Windows 2000 server crashes, the contents of its memory are copied out to disk. Because Windows 2000 supports up to 64 GB of physical RAM, a full memory crash dump can be quite slow, significantly delaying the system restart. For example, a Pentium Pro computer with 1 GB of memory takes approximately 20 minutes to dump memory to the paging file. When

the system reboots, it then takes an additional 25 minutes to copy dump data from the paging file to a dump file. This means that for 45 additional minutes, the system is unavailable.

For this reason, in addition to full-memory crash dumps, Windows 2000 also supports kernel-only crash dumps. These allow diagnosis of most kernel-related stop errors but require less time and space. The new feature is especially useful in cases where very large memory systems must be brought back into service quickly. Depending on system usage, a kernel-only crash dump can decrease both the size of the dump as well as the time required to perform the dump.

Using kernel-only crash dumps requires an administrative judgment call. Because essential data is sometimes mapped in user mode rather than kernel mode, and therefore can be lost using this method, administrators may choose to keep the full-memory crash dump mode on by default.

Mini Dumps

Similarly mini dump files contain specific information about application failures and enable applications to recover faster. With mini dump files, applications ascertain ways to fix problems automatically.

Faster CHKDSK

The CHKDSK command is used to check a hard disk for errors. Although CHKDSK is a powerful feature, it sometimes took hours to run depending on the file configuration of the disk partition being checked. Performance of CHKDSK in Windows 2000 has been enhanced significantly—up to 10 times faster, depending on the configuration.

MSINFO

The MSINFO tool generates system and configuration information. The MSINFO tool has been available for other Windows systems and is now offered on Windows 2000. MSINFO can be used to immediately determine the current system configuration, which is vitally important in troubleshooting any potential problems.

Remote Terminal Services

Remote Terminal Services are an integrated part of Windows 2000. These services allow administrators to view and manage their complete Windows 2000 environment from a single console. This capability makes it much easier to maintain the complete Windows

Windows 2000 Advanced Server Availability Features

2000 solution, which, in turn, significantly contributes to higher levels of availability and reliability.

Windows 2000 Advanced Server provides a powerful set of features designed to ensure that mission-critical applications and resources remain continuously available. This section introduces symmetric multiprocessing (SMP), clustering, network load balancing, and COM+ load balancing and shows how these technologies work together to enable high availability of critical applications, databases, and Web services.

Symmetric multiprocessing (SMP)

SMP lets software use multiple processors on a single server in order to improve performance, a concept known as hardware scaling, or scaling up. Any idle processor can be assigned any task, and up to 8 CPUs can be added to improve performance and handle increased loads. Improvements in the implementation of SMP code allow for improved scaling linearity, making Advanced Server a powerful platform for critical applications, databases, and Web services.

Clustering

Clustering provides users with constant access to important server-based resources. Windows 2000 Advanced Server provides the system services for two-node server clustering. With clustering, you create two cluster nodes that appear to users as one server. If one of the nodes in the cluster fails, the other node begins to provide service in a process known as failover. Combined with advanced SMP and large memory support in Windows 2000 Advanced Server, Windows clustering technologies enable organizations to ensure the availability of critical applications while being able to scale those applications both up and out to meet increased demand.

By providing redundant servers, clustering virtually eliminates most of the reliability issues with an individual server. Clustering addresses both planned sources of downtime—such as hardware and software upgrades—and unplanned, failure-driven outages. With Windows 2000 clustering, administrators can upgrade computers more efficiently by taking advantage of rolling upgrades. This lets you upgrade a machine in a cluster that is not handling user loads; when the upgrade is complete, users are switched to the upgraded machine. Rolling upgrades eliminate the need to reduce the availability of a server when software is upgraded.

Network Load Balancing

Another way to improve the availability of Windows 2000 systems is through the use of *network load balancing*. Network load balancing routes incoming requests to one of several different machines.

Network Load Balancing Services (NLBS) is implemented through the use of routing software associated with a single IP address. When a request comes into that address, it is transparently routed to one of the servers participating in load balancing.

NLBS is centered around multiple machines responding to requests to a single IP address. NLBS is especially important for building Web-based systems, where the demands of scalability and 24 x 7 availability require the use of multiple systems.

Load balancing, in conjunction with the use of “server farms,” is part of a scaling approach referred to as *scaling out*. The greater the number of machines involved in the load balancing scenario, the higher the throughput of the overall server farm. Load balancing also provides for improved availability, as each of the servers in the group acts as "live backup" for all the other machines participating in the load balancing. Windows 2000 NLBS is designed to detect and recover from the loss of an individual server in the group, which reduces maintenance costs while increasing availability.

Component Load Balancing

The newly released Microsoft Application Center 2000 will go beyond NLBS to include Component Load Balancing. With Component Load Balancing, Windows 2000 can balance loads among different instances of the same COM+ component running on one or more machines running Application Center 2000. Component Load Balancing is based on a usage algorithm, where a request is routed to the server that is either available or closest to being available when a request comes in. Component Load Balancing can be used in conjunction with Network Load Balancing Services. A system with Network Load Balancing Services, COM+ Load Balancing, and clustering is shown in Figure 2 below.

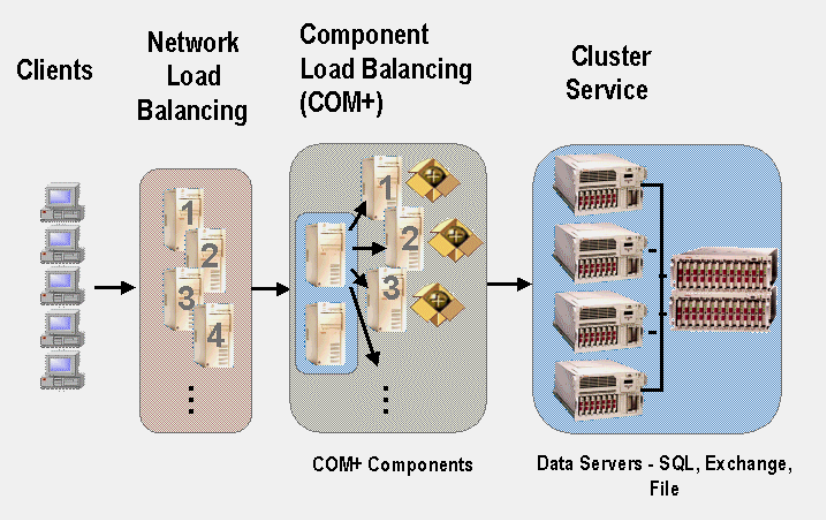

Figure 2 – A highly redundant system solution can combine Network Load Balancing, Component Load Balancing, and clustering.

Windows 2000 Datacenter Server expands the SMP and clustering features in Windows 2000 Advanced Server and includes new features to maximize reliability and availability. Datacenter Server is designed to meet the needs of online transaction processing (OLTP), large data warehouses, econometric analysis, large-scale simulations in science and engineering, and server consolidation.

Maximizing Availability: 32 SMP and 4-Node Clustering

Datacenter Server increases SMP capacity to 32 CPUs per cluster compared with 8 CPUs in Advanced Server. This allows network administrators to take full advantage of Network Load Balancing (NLB) capability. Failover support is increased in Datacenter Server to support four nodes, compared with two nodes in Advanced Server.

High Performance with Winsock Direct

In order to exploit the performance benefits of system area networks (SANs), Datacenter Server includes Winsock Direct, which streamlines communication between distributed components.

A system area network (SAN) is a particular class of network architecture that uses high-performance interconnections between secure servers to deliver reliable, high-bandwidth, low-overhead, and low-latency interprocess communications, usually within an IP subnet. SANs use switches to route data, with a typical hub supporting eight or more nodes and expanded to larger networks using cascading

hubs. Cable length limitations range from a few meters to a few kilometers.

Compared to a standard TCP/IP protocol stack on a local area network (LAN) of comparable line speed, deploying Winsock Direct enables efficient high-bandwidth, low-latency messaging that conserves processor time for application use. High-bandwidth and low-latency inter-process communication (IPC) and network system I/O allow more users on the system and provide faster response times and higher transaction rates.

Winsock Direct makes thousands of existing applications transparently SAN-enabled. As a result, the growth of SAN-based architectures in business-critical environments is expected to accelerate. Now developers of SAN interconnect hardware can develop interconnects that are compatible with Winsock Direct by using the Winsock Direct SAN infrastructure built in to Windows 2000 Datacenter Server.

Managing Critical Resources: The Process Control Tool

Process Control is a powerful, flexible tool that helps you manage and control the resources that processors use on your system by applying rules that you define. Process Control lets you customize an application's maximum memory use, application priority, application processor affinity and various other limits. When adjusted to fit the design of an application (placing limits only where an application is designed to handle such limits), Process Control helps ensure predictable and stable operations.

Maintaining optimum reliability and availability requires access to support professionals and programs specifically tailored for demanding business requirements. The most important support options for organizations include:

- **Microsoft Alliance Support.** This is designed to help very large enterprise customers successfully develop, deploy, and manage enterprise systems built around a broad range of high-quality Microsoft solutions for the server and the desktop. Alliance Support is available under two programs:
    - **Microsoft Alliance Support for Enterprise Systems** provides the highest level of attention available from

Microsoft, including personnel dedicated to the organization, the creation and management of exclusive information resources, and executive-level contact between the customer and Microsoft. For more information, see the complete fact sheet at http://support.microsoft.com/directory/factsheets/allenter.doc

- **Microsoft Alliance Support for High Availability** provides a fully personalized service that focuses not only on Microsoft Products but the hardware and environments in which they are deployed and the systems and operational processes by which they are managed. Microsoft and industry-leading service providers each contribute their strongest skills for this offering to provide a one-stop-shop for supporting a customer's complete IT environment built around Microsoft products and technologies. For more information, see the complete fact sheet at http://support.microsoft.com/directory/factsheets/allhigh.doc

- **Premier Support.** Provides proactive access to the professional services and technical expertise that large enterprises need to help maximize business value and minimize total cost. For more information on specific programs see:
  - Premier Support for the Enterprise http://support.microsoft.com/directory/factsheets/prement.doc
  - Microsoft Authorized Premier Support http://www.microsoft.com/support/mcsc/maps/

- **Professional Support.** This is Advanced support for experts and businesses using Microsoft products. For more information, see:
  - Customized support sites http://support.microsoft.com/directory/customer.asp
  - Online support requests for computer experts http://support.microsoft.com/directory/directory/onlinesrpro.asp
  - Professional Support Phone Numbers http://support.microsoft.com/directory/directory/phonepro.asp

Assisted Support Options for Organizations

Microsoft Certified Support Centers

Microsoft Certified Support Centers (MCSCs) are industry leading, multi-vendor support providers who have a special relationship with Microsoft that helps ensure they deliver high quality technical support for Microsoft products. All MCSCs possess significant industry expertise in many types of environments and can provide your organization with a broad range of life-cycle services and extended capabilities that form an economical and cohesive business solution. For more information on the support options available, see the Microsoft Certified Support Centers home page at http://www.microsoft.com/support/mcsc/

For a complete summary of support options, see the Support Options Overview page at http://support.microsoft.com/directory/overview.asp.

Windows 2000 Datacenter Program

The Windows 2000 Datacenter Program is designed to provide customers with an integrated hardware, software, and service offering—all delivered by Microsoft and qualified server vendors (OEMs). Three areas make up the program:

- **OEM/Microsoft Jointly Staffed Support Queue.** This gives partners access to the Microsoft resources they need to help customers achieve high levels of availability, and establishes a unique level of cooperation in delivering support for critical business systems.
- **Hardware Compatibility Test & List.** OEM products must pass a special Hardware Compatibility Test (HCT) verifying that quality hardware and software interacts efficiently and optimally with Microsoft products.
- **Software Maintenance.** Customers can receive update subscriptions for access to version releases, supplements, and Service Packs for Datacenter Server.

OEM/Microsoft Jointly Staffed Support Queue

Also known as the Microsoft Certified Support Center (MCSC) for Datacenter, this program gives partners access to the Microsoft resources they need to help customers achieve high levels of availability, and establishes a unique level of cooperation in delivering support for critical business systems. The jointly staffed support queue provides a comprehensive suite of services to help partners and Microsoft jointly deliver the service offerings that are needed for high-end environments using Windows 2000 Datacenter, including:

- Skills development and readiness services, such as advanced new product training; access to internships and special partner development programs at Microsoft; a partner-level knowledge base of known issues and resolution; early notification of critical problems and fixes; and, regular technical bulletins of support information.
- Software support services, including a joint team of Microsoft and partner support professionals to provide a single point of contact for customers; rapid escalation of critical or complex issues to Microsoft development for fixes; tools for managing hotfixes; and onsite critical problem support for customers.
- A source code license to help in the diagnosis and isolation of a problem.
- Business development services, including brand marketing, targeted joint marketing, customer satisfaction measurement, and participation in ongoing service development.
- Account management services, including a dedicated account manager, annual business planning assistance, and ongoing advocacy activities within Microsoft.

To be designated as an MCSC Datacenter partner, an organization must meet a series of qualifications as a service provider. Those qualifications include:

- Quality—consistent achievement of target customer satisfaction levels for support services provided to end customers and ongoing quality analysis and improvement methodologies.
- Staffing and certification—requirements for the number of full-time professionals that support Microsoft products and Microsoft certifications.
- Escalation—maximum rates for escalation of non-bug incidents to Microsoft and the ability to share support cases across partner

and Microsoft tracking systems.

- Problem replication environments—lab and replication environments capable of reproducing all Datacenter HCL systems for troubleshooting customer problems and testing software patches.
- IHV/ISV Escalation Path—24 x 7 access to an escalation path to debug resources and symbols files for all products certified as a part of the Datacenter system.
- Service offerings—the capability to provide service components including:
    - A minimum uptime guarantee of 99.9% availability.
    - Installation and configuration services.
    - Availability assessments.
    - 24 x 7 hardware and software support.
    - Response service for onsite hardware and software support.
    - Change management service.

Hardware Compatibility Test & List

OEM products must pass a special Hardware Compatibility Test (HCT) verifying that quality hardware and software interacts efficiently and optimally with Microsoft products. If successful, they're placed on the Hardware Compatibility List (HCL), and receive the "Designed for Windows" logo. The Windows logo on hardware products lets customers know the products meet Microsoft standards for compatibility with Windows operating systems. Hardware intended for use with Windows 2000 Datacenter Server must be designed to the specifications of the "Hardware Design Guide Version 2.0 for Microsoft Windows NT Server" at http://msdn.microsoft.com/library/books/serverdg/hardwaredesignguideversion20formicrosoftwindowsntserver.htm and the companion "Server Design FAQ" at http://www.microsoft.com/HWDEV/xpapers/SDG2FAQ/FAQ1.htm

All required specifications must be included in a Windows 2000 Datacenter server. In addition all Windows 2000 Datacenter servers must be capable of eight processors or more, although they can ship with fewer than eight processors.

Thus, customers who receive servers validated by the Windows Datacenter Program know that they are receiving a complete configuration that has been rigorously tested with all hardware components and kernel-level software products. Windows 2000 Datacenter Server will be provided only by OEMs who are willing to do extra testing and configuration control, and who can provide comprehensive customer support programs. The result is a highly reliable and dependable server. The testing that OEMs must do ensures the customer that the following components will work together smoothly on servers running Windows 2000 Datacenter Server:

- All hardware components.
- All hardware drivers.
- All software that works at the kernel level, including virus software, disk and tape management, backup software, and similar types of software.

The Role of Windows Hardware Quality Labs

Windows Hardware Quality Labs (WHQL) exist to ensure that OEMs produce quality hardware and software that interacts efficiently and optimally with Microsoft products. OEM products must pass the appropriate Hardware Compatibility Test (HCT).

Requiring a 14-day Test Period

As part of the certification process, Microsoft is requiring a 14-day test period to prove that servers running Windows 2000 Datacenter Server can meet or exceed 99.9% availability. This covers scheduled server availability. Microsoft established the 14-day test based on empirical studies of failures in Windows NT and Windows 2000 showing a mean recovery time of 20 minutes. To achieve 99.9% availability, therefore, a Windows 2000 Datacenter Server must have a mean time between failures (MTBF), under normal customer load, of 13.875 days. Microsoft designed the Windows 2000 Datacenter Server test to be three times normal customer load; this means that the MTBF under test load must meet or exceed 4.625 days. (Extensive reliability research has shown that the MTBF is directly related to *execution time,* not *calendar time;* therefore, the test can be accelerated by increasing the load.)

To demonstrate that a Windows 2000 Datacenter Server–based system meets the desired MTBF, the system must run under test, with zero failures, for the amount of time determined by the formula **-(tMTBF)*(ln r)**. *tMTBF* is the threshold MTBF--in this case, 4.625

days. r is the risk that the test will incorrectly accept a system. For this test, the risk level is 5% ($r = 0.05$). According to the formula, a Windows 2000 Datacenter Server system must run under test, without failure, for 14 days.

Ongoing Testing Requirements

Windows 2000 Datacenter–based servers are required to resubmit configuration files and test results for each Microsoft Windows Service Pack or any driver service changes provided by the vendor. When the new Windows 2000 Datacenter program configuration is available, the previous configuration remains valid. Upgrading to a new configuration and Service Pack should be done after the customer has reviewed their requirements and system availability with their system partners.

Datacenter Planning

The key to installing and maintaining highly reliable Windows 2000 Datacenter Server-based systems is good initial planning, operating procedures and change control. Before installing a Windows 2000 Datacenter Server customers and their vendors should do the following:

- Identify workloads and servers you are going to run with Windows 2000 Datacenter Servers.
- Determine the specific hardware configuration for these Windows 2000 Datacenter servers including all required adaptors.
- Identify all the installed non-Microsoft kernel drivers required for these systems.
- Work with your system supplier to create a Windows 2000 Datacenter program configuration.
- Identify your QFE and Service Pack plans and policies.
- Ensure your change control and operation procedures for maintaining Windows 2000 Datacenter program configurations are in place.

After identifying the configuration you require, work with your system supplier to receive a Windows 2000 Datacenter program configuration. Windows 2000 Datacenter program configuration files are available on the WHQL site of Microsoft.com at

http://www.microsoft.com/hwtest/default.asp or your system supplier and can be downloaded to check your systems.

Windows 2000 Datacenter Program Servers

At a minimum, servers running Windows 2000 Datacenter Server must contain the following hardware or features:

- Minimum CPU speed 400 MHz.
- Intelligent RAID storage subsystem.
- 512K L2 cache or equivalent memory for single processor systems; 256K L2 cache per processor minimum of 2P and greater systems.
- Expansion to at least eight processors.
- Minimum 2 GB expandable to 4 GB.
- System memory includes ECC memory protection.
- Support 64-bit bus architecture including 64-bit physical address space, 64-bit PCI adapters must be able to address any location in the address space supported by the platform and 64-bit processors.
- SCSI host controller or fiber channel adaptor.
- Power supply protection using N+1 (extra unit).
- Support for replacement of power supplies.
- Local hot-swap power supply replacement indicators.
- Support for replacement of fans.
- Support for multiple hard drives.
- RAID subsystem supports automatic replacement of failed drive.
- RAID subsystem supports manual replacement of failed drive.
- Support for at least one of RAID 1, 5, or 10.
- Alert indicators for imminence of failure.
- Alert indicators for occurrence of failure.

For more information about Windows Hardware Quality Labs and the Hardware Compatibility Test, see “The Windows Datacenter Program: Ensuring Hardware Quality” at http://www.microsoft.com/windows2000/guide/datacenter/hcl/dchclprogram.asp

People and Process

Software Maintenance

Customers of Windows 2000 Datacenter Server can choose to receive updateable subscriptions for the operating system from the OEM. The update subscriptions provide access to version releases, supplements, and Service Packs for Datacenter Server. The subscription is available on a monthly or yearly basis, and a customer must continue to renew the subscription with the OEM to obtain the benefits of the subscription.

Microsoft Operations Framework: Roadmap for Reliability

Studies show that as much as 80 percent of system failures can be traced to errors caused by people or processes. Therefore, an essential part of reliability strategy is adopting and following prescriptive guidelines that cover the best practices that have been learned by enterprises over time. The Microsoft Operations Framework (MOF) provides technical guidance for achieving mission-critical production system reliability, availability, and manageability on Microsoft products and technologies.

Building on Standardized Best Practices

MOF recognizes that the current industry best practice for IT service management has been well documented within the Central Computer and Telecommunications Agency’s (CCTA) IT Infrastructure Library (ITIL).

The CCTA is a United Kingdom government executive agency chartered with development of best practice advice and guidance on the use of information technology in service management and operations. To accomplish this, the CCTA charters projects with leading information technology companies from around the world to document and validate best practices in the disciplines of IT service management.

MOF combines these collaborative industry standards with specific guidelines for using Microsoft products and technologies. MOF also extends ITIL code of practice to support distributed IT environments and current industry trends such as application hosting and Web-based transactional and e-commerce systems.

Enterprise Services Frameworks

MOF is one of the three frameworks that form Enterprise Services Frameworks (ESF). Each ESF framework targets a different, but integral, phase in the information technology (IT) life cycle. Each

framework provides useful and detailed information on the people, processes, and technologies required to successfully execute within its respective area. The other two ESF frameworks are Microsoft Readiness Framework (MRF) and the Microsoft Solutions Framework (MSF). Figure 3 below shows how each of the frameworks fits into ESF.

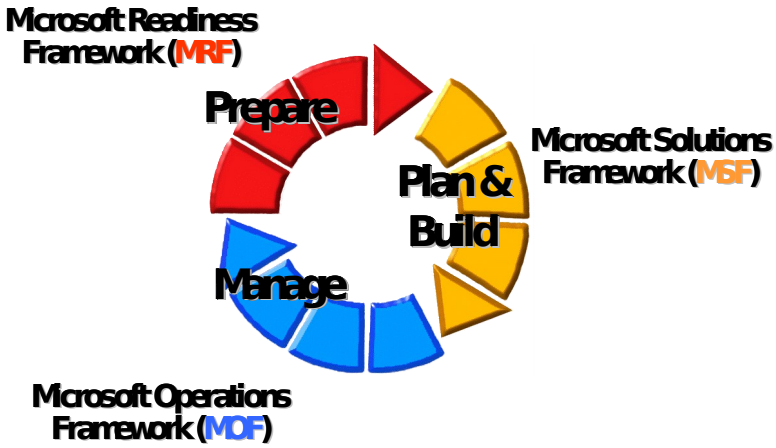

Figure 3. Enterprise Services Frameworks

The Microsoft Operations Framework includes a comprehensive suite of operational guidance in the form of white papers, operations guides, assessment tools, operations kits, best practices, case studies, and support tools that address the people, process, and technologies for effectively managing production systems within today's complex distributed IT environment. For more information on Microsoft's enterprise frameworks and offerings, see:

- Microsoft Solutions Framework home page at http://www.microsoft.com/msf
- Microsoft Operations Framework white papers at http://www.microsoft.com/trainingandservices/MOFoverview

Principles of MOF

Key to Design and Application

MOF addresses the dynamic, ever-changing nature of today's distributed IT environments. This framework consists of six principles that are fundamental in its design and key to its successful application. Table 1 below lists these principles and how MOF uses them.

Table 1. Microsoft Operations Framework Principles

Principle	Description
IT/ business alignment	Design IT services to meet business goals and priorities.
Customer focused	Use service level agreements (SLAs) to manage the quality of customer services.
Spiral life cycle	Continuously assess and adapt operations services.
Team of peers	Organize the communication, skills, roles, and responsibilities of a highly competent and flexible operations staffing model.
Best practices	Leverage industry and Microsoft best practices.
Measurement	Develop and use tools to measure operations activities.

The MOF Process Model

A Simplified Approach

Defining any high-level process model requires a compromise that balances simplicity and understanding with scientific accuracy. IT operations is a complex set of dynamics that would be a challenge for anyone to capture accurately. With so many processes, procedures, and communications happening simultaneously across a diverse set of systems, applications, and platforms, it is virtually impossible to model exactly.

As a result, MOF's approach is to simplify this complex set of dynamics into a framework that is easy to understand and whose principles and practices are easy to incorporate and apply. The power of this simplified approach will enable the operations staff of an enterprise of any size, regardless of maturity level, to realize tangible benefits to the existing, or proposed, operations.

The MOF process model has four main concepts that are key to understanding the model:

- IT service management, like software development, has a life cycle.

- The life cycle is made up of distinct logical phases that run concurrently.
- Operations reviews must be both release based and time based.
- IT service management touches every aspect of the enterprise.

With this understanding, the MOF process model consists of four integrated phases. They are:

- Changing
- Operating
- Supporting
- Optimizing

These phases form a spiral life cycle that can be applied to a specific application, a data center or an entire operations environment with multiple data centers, including outsourced operations and hosted applications.

Each phase culminates with a review milestone specifically tailored to assess the operational effectiveness of the preceding phase. These phases, coupled with their designated review milestones, work together to meet organizational goals and objectives. Figure 4 below illustrates the MOF process model and the relationship of the life cycle phases, the reviews following each phase, and the concept of IT service management at the core of the model. The figure depicts each phase of the IT operation connected in a continuous spiral life cycle.

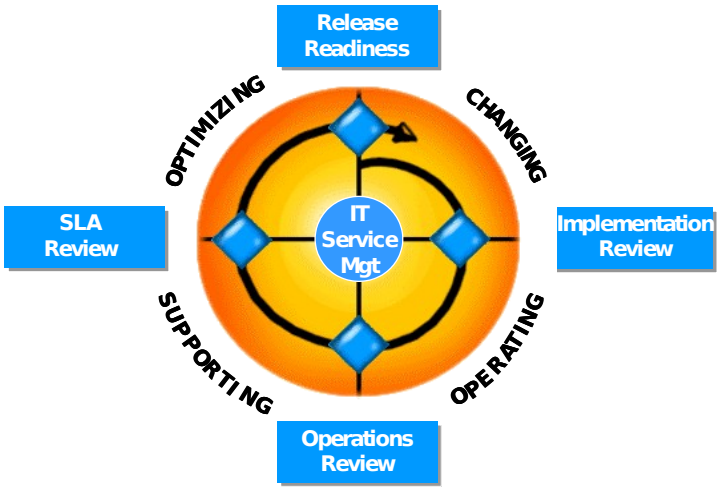

Figure 4. The MOF Process Model

The process model incorporates two types of review milestones—release based and time based. Two of the four reviews—release readiness and implementation—are release based and occur at the introduction of a release into the target environment. The remaining two reviews—operations and service level agreement—occur at regular intervals to assess the internal operations as well as the customer service levels.

The reason for this mix of review types within the process model is to support two concepts necessary in a successful IT operations environment:

- The need to manage the introduction of change through the use of managed releases. Managed releases allow for a clear packaging of change that can then be identified, tracked, tested, implemented, and operated.
- The need to continually assess and adapt the operational procedures, processes, tools, and people required to deliver the specific service solutions. The time-based review supports this concept.

The following table summarizes the key activities and subsequent review for each of the four phases:

Phase	Activities	Review
Changing	Introduce new service solutions, technologies, systems, applications, hardware, and processes	Implementation
Operating	Execute day-to-day tasks effectively	Operations
Supporting	Resolve incidents, problems, and inquiries quickly	Service level agreement
Optimizing	Optimize cost, performance, capacity, and availability	Release readiness

The MOF process model promotes a high level of availability, reliability, and manageability. For this reason, IT managers will find the MOF process model useful in the following environments:

- Production
- Production certification
- User acceptance
- Prerelease or staging
- Integration or system test

Investing in properly trained or certified personnel

The potential for human error remains a significant roadblock in keeping your systems reliable and available. People may forget to perform backups or ignore proper procedures for performing a wide range of operational tasks. The lesson is clear: If your employees aren't properly trained to maintain your systems, you risk compromising the reliability and availability that you should be achieving. Two extensive programs exist to help you meet this goal: The Microsoft Readiness Framework and the Microsoft Certification Program.

Microsoft Readiness Framework

The Microsoft Readiness Framework helps IT organizations develop individual and organizational readiness to use Microsoft's products and technologies. This guidance includes assessment and readiness planning tools, learning roadmaps, readiness-related white papers, self-paced training, courses, certification exams, and readiness events.

MRF offers a structured approach to reliably and efficiently assess the technical requirements (both individual and organizational) necessary to plan, build, and manage solutions. The framework provides capability planning, organizational competency identification, and individual and organizational assessments.

For more information about how MRF fits in with the Enterprise Services Framework, see the Enterprise Services home page at http://www.microsoft.com/msf.

Microsoft Certification

Competitive organizations are led at all levels by professionals who know technology and can innovate, take initiative, and think strategically. Microsoft certification can help organizations find these technical leaders.

Microsoft certification is an objective way for businesses to identify individuals who have the technical abilities to help them compete in their industry and move forward with the most advanced Microsoft technology. Certification provides professionals with a credential that acknowledges their skills with Microsoft products.

For more information about Microsoft certification and other training opportunities, see the Microsoft Certification Web site at http://www.microsoft.com/trainingandservices/default.asp

Appendix A: Reduced Reboot Scenarios

For information about a wide range of learning services for Windows 2000 including online courses, seminars, and courseware about specific technologies, see the Windows 2000 Learning Center at http://www.microsoft.com/trainingandservices/default.asp?PageId=training&LearnCenterHtm=win2000

The Windows 2000 Server product line is the most reliable set of server operating systems Microsoft has ever produced. The reliability improvements in Windows 2000 mean fewer network interruptions for end users, higher server uptime, and better availability.

Advanced Server meets the needs of essential business and e-commerce applications that handle heavier workloads and high-priority processes. You can readily increase your server capacity to keep pace with business growth while enhancing the availability of your important systems.

Windows 2000 Datacenter Server uses stringent standards for hardware and software configurations to deliver an OS designed to meet the highest demands for reliability and availability. It includes all features in Advanced Sever plus greater clustering, load balancing, memory support, process controls, and other features optimized to deliver the high availability and reliability required for enterprise and larger departmental solutions.

This dependability is further enhanced by the Windows 2000 Datacenter Program, giving customers an integrated hardware, software, and service offering—all delivered by Microsoft and qualified server vendors (OEMs).

Obtaining optimum reliability and availability depends on investments in people and process, ensuring properly trained personnel follow prescriptive practices based on the Microsoft Operations Framework and the expertise provided by support programs.

The following tasks no longer require rebooting your system.

File system maintenance

- Extending an NTFS volume.
- Mirroring an NTFS volume.

Hardware installation and maintenance

- Docking or undocking a laptop computer.
- Enabling or disabling network adapters.
- Installing or removing Personal Computer Memory Card International Association (PCMCIA) devices.
- Installing or removing Plug and Play disks and tape storage.
- Installing or removing Plug and Play modems.
- Installing or removing Plug and Play network interface controllers.
- Installing or removing the Internet Locator Service.
- Installing or removing Universal Serial Bus (USB) devices, including mouse devices, joysticks, keyboards, video capture, and speakers.

Networking and communications

- Adding or removing network protocols, including TCP/IP, IPX/SPX, NetBEUI, DLC, and AppleTalk.
- Adding or removing network services, such as SNMP, WINS, DHCP, and RAS.
- Adding Point-to-Point Tunneling Protocol (PPTP) ports.
- Changing IP settings, including default gateway, subnet mask, DNS server address, and WINS server address.
- Changing the Asynchronous Transfer Mode (ATM) address of the ATMARP server. (ATMARP was third-party software on Windows NT 4.)
- Changing the IP address if there is more than one network interface controller.
- Changing the IPX frame type.
- Changing the protocol binding order.
- Changing the server name for AppleTalk workstations.
- Installing Dial-Up Server on a system with Dial-Up Client installed and RAS already running.
- Loading and using TAPI providers.
- Resolving IP address conflicts.

Appendix B: Tools for Third Parties

- Switching between static and DHCP IP address selections.
- Switching MacClient network adapters and viewing shared volumes.

Memory management

- Adding a new PageFile.
- Increasing the PageFile initial size.
- Increasing the PageFile maximum size.

Software installation

- Installing a device driver kit (DDK).
- Installing a software development kit (SDK).
- Installing Internet Information Service.
- Installing Microsoft Connection Manager.
- Installing Microsoft Exchange 5.5.
- Installing Microsoft SQL Server™ 7.0.
- Installing or removing File and Print Services for NetWare.
- Installing or removing Gateway Services for NetWare.

Performance tuning

- Changing performance optimization between applications and background services.

Windows 2000 also provides a number of tools and features that make it easier for independent software vendors to write dependable code for Windows 2000.

Kernel-Mode Code Development

As described earlier, software can be categorized into two major types of code: user-mode code, which includes application software such as a spreadsheet program; and kernel-mode code, such as core operating system services and device drivers. Development tools that help programmers write reliable application code aren’t necessarily appropriate for developers writing kernel-mode code. Because writing kernel-mode code presents special challenges, Windows 2000 Server includes tools for kernel-mode developers.

Device drivers, often simply referred to as drivers, are the kernel-mode code that connects the operating system to hardware, such as video cards and keyboards. To maximize system performance, kernel-mode code doesn't have the memory protection mechanisms used for application code. Instead, this code is trusted by the operating system to be free of errors. In order to safely interact with other drivers and operating system components, drivers and other kernel-mode code must follow complex rules. A slight deviation from these rules can result in errant code that can inadvertently corrupt memory allocated to other kernel-mode components.

Some kernel-mode code errors show up immediately during testing. But other types of errors can take a long time to cause a crash, making it difficult to determine where the problem originates. In addition, it is not easy for driver developers to fully test kernel-mode code because it is difficult to simulate all the workload, hardware, and software variables that might be encountered in a production environment.

To address these issues, Windows 2000 Server includes the following features and tools to help developers produce better drivers:

- Pool Tagging
- Driver Verifier
- Device Path Exerciser

Pool Tagging

The Windows NT 4.0 kernel contains a fully shared pool of memory that is allocated to tasks and returned to the pool when no longer needed. Although using the shared memory pool is an efficient way of using memory in a run-time system, the shared pool can create problems for driver developers if they make a mistake in their code.

One common error is to let a kernel-mode component write outside of its memory allocation. This action can corrupt the memory of another kernel-mode component and cause a system failure.

Another common mistake is to allocate memory for a driver process and then fail to release it when the process is finished, creating a *memory leak*. Memory leaks slowly consume more and more memory and eventually exhaust the shared memory pool, which causes the system to fail. This scenario may take a long time to develop. For example, a driver that requests a small amount of memory and only

forgets to release that memory in rare situations will take a long time to exhaust the memory pool.

Both types of errors can be hard to track down. To help developers find and fix such memory problems, *Pool Tagging* (also known as the *Special Pool*), has been added to Windows 2000. For testing purposes, Pool Tagging lets kernel-mode device driver developers make all memory allocations to selected device drivers out of a special pool, rather than a shared system pool. The end of the special pool is marked by a Guard Page. If an application tries to write beyond the boundary of their memory allocation, it hits a Guard Page, which causes a system failure. Once alerted by the system failure, a developer can track down the cause of the memory allocation problem.

To help developers find memory leaks, Pool Tagging also lets developers put an extra tag on all allocations made from the shared pool to track tasks that make changes to memory.

Driver Verifier

The Driver Verifier is a series of checks added to the Windows 2000 kernel to help expose errors in kernel-mode drivers. The Driver Verifier is ideal for testing new drivers and configurations for later replication in production. These checks are also useful for support purposes, such as when a particular driver is suspected as the cause of crashes in production hardware. The Driver Verifier also includes a graphical user interface tool for managing the Driver Verifier settings.

The Driver Verifier tests for specific sets of error conditions. Once an error condition is found, it is added to the existing suite of tests for future testing purposes. The Driver Verifier can test for the following types of problems:

- **Memory corruption.** The Driver Verifier checks extensively for common sources of memory corruption, including using uninitialized variables, double releases of spinlocks, and pool corruption.
- **Writing to pageable data.** This test looks for drivers that access pageable resources at an inappropriate time. The problems that result from these types of errors can result in a fatal system error, but may only appear when a system is handling a full production workload.
- **Handling memory allocation errors.** A common programming error is neglecting to include adequate code in the driver to handle a situation when the kernel cannot allocate the

memory the driver requests. The Driver Verifier can be configured to inject random memory allocation failures to the specified driver, which allows developers to quickly determine how their drivers will react in this type of adverse situation.

Because Driver Verifier impacts performance, it shouldn't be used continuously, or in a production environment. Developer guidelines for using Driver Verifier are published at http://www.microsoft.com/hwdev/driver/driververify.htm.

Device Path Exerciser

The Device Path Exerciser tests how a device driver handles errors in code that use the device. It does this by calling the driver, synchronously or asynchronously, through various user-mode I/O interfaces and testing to see how the driver handles mismatched requests. For example, it might connect to a network driver and ask it to rewind a tape. It might connect to a printer driver and ask it to re-synchronize the communication line. Or, it might request a device function with missing, small, or corrupted buffers. Such tests help developers make their drivers more robust under error conditions, and improve drivers that cannot handle the tested calls properly.

Devctl, the Device Path Exerciser, ships in the Hardware Compatibility Test 8.0 test suite, available at http://www.microsoft.com/hwtest/TestKits/

Driver Signing

In addition to the tools provided for driver developers, Microsoft has also added a way to inform users if the drivers they are installing have been certified by the Microsoft testing process.

Windows 2000 includes a new feature called Driver Signing. Driver Signing is included in Windows to help promote driver quality by allowing Windows 2000 to notify users whether or not a driver they are installing has passed the Microsoft certification process. Driver Signing attaches an encrypted digital signature to a code file that has passed the Windows Hardware Quality Labs (WHQL) tests.

Microsoft will digitally sign drivers as part of WHQL testing if the driver runs on Windows 98 and Windows 2000 operating systems. The digital signature will be associated with individual driver packages and will be recognized by Windows 2000. This certification proves to users that the drivers they employ are identical to those Microsoft has tested, and notifies users if a driver file has been changed after the driver was put on the Hardware Compatibility List.

If a driver being installed has not been digitally signed, there are three possible responses:

- **Warn:** lets the user know if a driver that's being installed hasn't been signed and gives the user a chance to say "no" to the install. Warn will also give the user the option to install unsigned versions of a protected driver file.
- **Block:** prevents all unsigned drivers from being installed.
- **Ignore:** allows all files to be installed, whether they've been signed or not.

Windows 2000 will ship with the Warn mode set as the default.

- Vendors wishing to have drivers tested and signed can find information on driver signing at http://www.microsoft.com/hwtest/. Only signed drivers are published on the Windows Update Web site at http://windowsupdate.microsoft.com/default.htm

Developing and debugging user-mode code

User mode is the portion of the operating system in which application software runs. Windows 2000 includes a new tool, PageHeap, which can help developers find memory access errors when they are working on non-kernel-mode software code.

Heap refers to the memory used to temporarily store code. *Heap corruption* is a common problem in application development. Heap corruption typically occurs when an application allocates a block of heap memory of a given size and then writes to memory addresses beyond the requested size of the heap block. Another common cause of heap corruption is writing to a block of memory that has already been freed. In both cases, the result can be that two applications try to use the same area of memory, leading to a system failure. To help developers find coding errors in memory buffer use faster and more reliably, the PageHeap feature has been built into the Windows 2000 heap manager.

When the PageHeap feature is enabled for an application, all heap allocations in that application are placed in memory so that the end of the heap allocation is aligned with the end of a virtual page of memory. This arrangement is similar to the tagged pool described for kernel memory. Any memory reads or writes beyond the end of the heap allocation will cause an immediate access violation in the

For More Information

application, which can then be caught within a debugger to show the developer the exact line of code that is causing heap corruption.

For the latest information on Windows 2000, check out our Web site at http://www.microsoft.com/windows2000 and the Windows 2000/NT Forum at http://computingcentral.msn.com/topics/windowsnt.

See also:

Windows 2000 Server and Advanced Server home page:
http://www.microsoft.com/windows2000/server

Windows 2000 Datacenter Server home page:
http://www.microsoft.com/windows2000/datacenter

Microsoft Application Center 2000 home page:
http://www.microsoft.com/applicationcenter/

Introduction to reliability and availability in Windows 2000 Server:
http://www.microsoft.com/windows2000/guide/server/overview/reliable/default.asp

Microsoft Press Windows 2000 resources:
http://mspress.microsoft.com/Windows2000

Microsoft Support options page:
http://support.microsoft.com/directory/overview.asp.

Microsoft Certified Support Centers home page:
http://www.microsoft.com/support/mcsc/

Microsoft Enterprise Services home page:

http://www.microsoft.com/msf

Microsoft Operations Framework white papers:
http://www.microsoft.com/trainingandservices/MOFoverview

Microsoft Certification home page:
http://www.microsoft.com/trainingandservices/default.asp

Hardware Design Guide Version 2.0 for Microsoft Windows NT Server:
http://msdn.microsoft.com/library/books/serverdg/hardwaredesignguideversion20formicrosoftwindowsntserver.htm

Server Design FAQ:
http://www.microsoft.com/HWDEV/xpapers/SDG2FAQ/FAQ1.htm

Microsoft Windows Hardware Quality Labs home page:
http://www.microsoft.com/hwtest/default.asp